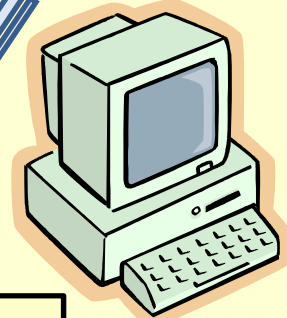
資料3

スマートフォンのセキュリティについて

平成23年5月12日
総務省総合通信基盤局
電気通信事業部
消費者行政課

携帯電話とスマートフォンの相違について

スマートフォンの性格が、携帯電話の高機能化したものとのイメージが先行し、スマートフォンの基本的性格（セキュリティの必要性等）を見落とすおそれがある。

携帯電話、スマートフォン、PCの位置づけ

携帯電話、スマートフォン、PCの事業モデルの相違

○ 事業モデル		
従来の携帯電話	スマートフォン	PC
通信事業者による端末／OS／アプリ／通信をクローズドに管理・一元的に利用者に提供 （垂直統合型）	基本的に端末／OS／アプリ／通信をオープン化して役割分担 （垂直統合型～水平展開型の形態が存在）	端末／OS／アプリ／通信をオープン化して役割分担 （水平展開型）
○ 総合的な安全度		
従来の携帯電話 ＞ スマートフォン ＞ PC		

○スマートフォンは、従来の携帯電話（フィーチャーフォン）よりもPCの特徴に近い部分（図中白色の部分）が多い。

項目＼商品	携帯電話：～フィーチャーフォン	携帯電話：スマートフォン		PC
電話機能	3G接続			ソフトフォン
可搬性	片手操作	5インチ程度	タブレット	～DESKTOP
インターネット接続先	通信事業者網経由	一般サイトISP経由		一般サイトISP経由
端末PF	組込みソフト	オープンPF		汎用OS
ダウンロード（DL）アプリ	APIにより機能は限定	アプリの自由度は大きい		アプリの自由度は大きい
セキュリティ対策	通信事業者がNW対応		セキュリティソフト組み込み／ISPで設定等	

電気通信サービス利用者WG第5回において（一社）情報通信ネットワーク産業協会から提出された資料から抜粋

※スマートフォンと呼ばれる端末の各機能は現時点では明確に分けられないので、表は大まかな位置づけとして記載。

スマートフォンの安全度等の比較

主なスマートフォンの安全度等の比較

○　主なOS		
AndroidOS	iOS	BlackBerryOS
○　OSの設計思想		
オープン化	クローズド	クローズド
○　ネットワーク		
インターネット網	インターネット網	閉域網（暗号化措置）
○　アプリの提供状況		
・アプリの開発は誰でも可能 ・アプリを掲載する際の事前審査なし ・利用者・技術者等からの申告を踏まえ、マルウェアが見つかり次第アプリをOSベンダーが削除	OSベンダーがアプリを事前に審査実施し、安全性を確認したアプリをApp Storeで提供	（法人の場合）管理者が許可しないアプリはインストール不可
○　利用者から見た機能拡張の自由度の比較		
AndroidOS　＞　iOS　＞　BlackBerryOS		
○　安全度の比較		
AndroidOS　＜　iOS　＜　BlackBerryOS		
（備考）各OS搭載端末を扱っている事業者		
ドコモ、au、SBM	SBM	ドコモ

スマートフォンの利用に存在するリスク

〇スマートフォンは、機能的・構造的にPCに近い特徴を有しており、PCと同様にマルウェアの標的となりやすい。

１　マルウェアのリスクの高まる要因

- OSがより普及して、対象端末台数が増加。
- オープンな設計思想により、OSなど端末プラットフォームの情報を入手でき、より詳細な制御をアプリ側から行うことが可能。
- 一般のサイト等からの不特定のアプリケーションのインストールが可能。

２　マルウェアの検出状況

- PCでは多くのマルウェアが確認されているが、現状では、スマートフォンに関してはPCに比べればわずか。
- しかし、今後のスマートフォンの普及により、マルウェアの増加は確実視されている。

３　マルウェアへの対応状況

- アプリのインストール時にそのアプリの機能が表示され、それに対しユーザが承認を与える仕組みが用意されているOSがあるが、機能の表示のみでは、アプリの良性・悪性の自己判断は困難な場合が多い。
- スマートフォン用のセキュリティ対策ソフトは普及半ば。

〇大容量のデータ蓄積が可能

紛失時、故障時のデータ喪失の懸念
端末廃棄時におけるデータ流出のおそれ

スマートフォンのセキュリティに関する取組

セキュリティベンダーの取組

○ スマートフォン向けのセキュリティソフトの提供（Norton Mobile Security for Android、Kaspersky Mobile Security 9、McAfee Virus Scan Mobile for Android）
○ スマートフォン向けポータルサイトの設置、スマートフォンセキュリティセミナーの実施（法人向け）
○ セキュリティソフトのプリインストールの検討　等

端末メーカの取組

○ 取扱説明書において、アプリのインストールは自己責任であることを周知

携帯電話事業者の取組（アンドロイド・個人向け）

○ 独自に事前審査したアプリケーションを利用者に提供するアプリマーケットを設置
○ 取扱説明書などにウィルスへの感染の危険性について記載
○ セキュリティ関係サービスの提供、セキュリティ対策ソフトの提供と利用者への周知

ドコモ	KDDI	SBM
○ アプリの審査		
Docomo marketで提供されるアプリについては、ドコモが事前審査	au one marketで提供されるアプリについては、KDDIが事前審査	－
○ セキュリティ関係サービス		
・アクセス制限サービス（spモード利用時） ・メールウイルスチェック（spモード利用時）	・フィルタリングサービス ・安心ロック、遠隔ロック	・ウェブ利用制限 ・スマートセキュリティ powered by McAfee® ・紛失ケータイ捜索サービス（スマートフォン基本パックにて提供） ・あんしん設定アプリ
○ 利用者への周知		
端末の取扱説明書に、アプリのインストールに対する注意事項を記載。	端末の取扱説明書にウィルスへの感染等について注意喚起。ショップにおいて口頭説明。	購入の際に契約者に渡す文書に、ウィルスへの感染の危険性について記載し、対策ソフトの利用を案内。

スマートフォンに関する検討課題

課題

○スマートフォン普及に伴い、新たに発生する問題点（セキュリティに関する事項、事業者対応の限界等）を整理し、携帯電話との相違点について、利用者周知を行うべきではないか。

○スマートフォンのセキュリティ確保のため、専門家による検討を進める必要があるのではないか。

現状

○　スマートフォンは、機能的・構造的にPCに近い特徴を有しているため、従来の携帯電話が「高機能化」したものではなく、「電話機能が付いたPC」と見るべき（スマートフォンでは、従来の携帯電話サービスで利用できたサービスの全てが利用できるものではない。）。

○　また、従来型の携帯電話と異なり、スマートフォンのOSは、PC同様にマルウェアの攻撃対象となりやすいことから、電気通信サービスの利用時において、新たな問題が生じるおそれがある。

○　しかし、こうした従来の携帯電話とスマートフォンの基本的な相違点については、利用者周知が十分になされていない現状にある。

○　また、利用者側においても、スマートフォンを利用するに当たっては、従来の携帯電話の利用に比べて高いリテラシーが求められていることの認識が必要。

○　スマートフォンの普及により、マルウェアの増加は確実視されていることを踏まえ、セキュリティベンダー、端末ベンダー、携帯電話事業者など関係する事業者では、利用者への周知やスマートフォン向けのセキュリティサービスの提供などの取組を開始している。

○　スマートフォンの利用に伴う問合わせ等については、電気通信事業者は適切に対応することがもとめられるが、端末の購入ルートの多様化に伴い、対応できない状況に直面しているとの指摘がある。